Claims

What is claimed is:

1. A method for maintaining a password in a computer system equipped with an operating system for running a dedicated application, comprising:

generating a password in response to an occurrence of a prescribed password generation event;

providing the generated password to an operating system security module;

producing a coded password as a function of the generated password; and

storing the coded password for use in connection with a secure operating system login access.

2. The method of claim 1, wherein providing the generated password to the operating system security module further includes overwriting a previously generated password.

3. The method of claim 1, wherein storing the coded password further includes overwriting a previously stored coded password.

4. The method of claim 1, further comprising:

displaying the stored coded password during an operating system login, wherein the displayed coded password is subject to being decoded with the use of a corresponding secure password provider, further wherein the secure operating system login is responsive to an input of a correctly decoded coded password for enabling access to the operating system as a function of the generated password and the operating system security module.

5. The method of claim 1, wherein the prescribed password generation event includes at least one selected from the group consisting of a computer system power-up; a computer system re-boot; expiration of a prescribed time duration from an immediately preceding password generation event; restoration of a security level from a modified security level to a default security level, and occurrence of a secure operating system login access.

6. The method of claim 5, wherein the modified security level of a password generation event includes at least one selected from the group consisting of a change in the security level within the dedicated application, a security level override within the dedicated application, and a one-shot security access within the dedicated application.

7. The method of claim 1, further comprising:

searching a username registry of the dedicated application upon the occurrence of the prescribed password generation event and removing any invalid usernames from the username registry.

8. The method of claim 7, further comprising:

reviewing privileges associated with respective valid usernames in the username registry and resetting the privileges of the respective valid username to prescribed default settings.

9. The method of claim 1, wherein generating the password includes generating the password for a prescribed username.

10. The method of claim 9, wherein the prescribed username includes a service username.

11. The method of claim 1, wherein the dedicated application includes a point of sale application in a fuel dispensing environment.

12. The method of claim 1, wherein the computer system includes at least one selected from the group consisting of a stand-alone computer system and a stand-alone network of computer systems.

13. A computer system having a password maintenance capability comprising:

an operating system including an operating system security module, an operating system data store module, and an operating system login module, said operating system operable for executing a dedicated application; and

a password security generator including a password generator and a password encryptor, wherein

the password generator couples with said operating system for generating a password in response to an occurrence of a prescribed password generation event, the password generator providing the generated password to the operating system security module, and

the password encryptor couples to the password generator for producing a coded password as a function of the generated password, the password encryptor providing the coded password to the operating system data store module for use in connection with a secure operating system login access via the operating system login module.

14. The computer system of claim 13, wherein further the password generator provides the generated password to the operating system security module and overwrites a previously generated password.

15. The computer system of claim 13, wherein further the password encryptor stores the coded password and overwrites a previously stored coded password.

16. The computer system of claim 13, further comprising:

means for displaying the stored coded password during an operating system login, wherein the displayed coded password is subject to being decoded with the use of a corresponding secure password provider, further wherein the operating system login module is responsive to an input of a correctly decoded coded password for enabling access to said operating system as a function of the generated password and the operating system security module.

17. The computer system of claim 13, wherein the prescribed password generation event includes at least one selected from the group consisting of a computer system power-up; a computer system re-boot; expiration of a prescribed time duration from an immediately preceding password generation event; restoration of a security level from a modified security level to a default security level, and occurrence of a secure operating system login access.

18. The computer system of claim 17, wherein the modified security level of a password generation event includes at least one selected from the group consisting of a change in the security level within the dedicated application, a security level override within the dedicated application, and a one-shot security access within the dedicated application.

19. The computer system of claim 13, further wherein said password security generator further includes means responsive to an occurrence of a prescribed password generation event for searching a username registry of the dedicated application and removing any invalid usernames from the username registry.

20. The computer system of claim 19, further wherein the searching means reviews privileges associated with respective valid usernames in the username registry and resets the privileges of the respective valid username to prescribed default settings.

21. The computer system of claim 13, wherein the password generator generates the password for a service username.

22. The computer system of claim 13, wherein the dedicated application includes a point of sale application in a fuel dispensing environment.

23. The computer system of claim 13, wherein said computer system includes at least one selected from the group consisting of a stand-alone computer system and a stand-alone network of computer systems.

24. A computer program product for maintaining a password in a computer system equipped with an operating system for running a dedicated application, comprising:

a computer program processable by a computer system for causing the computer system to:

generate a password in response to an occurrence of a prescribed password generation event,

provide the generated password to an operating system security module,

produce a coded password as a function of the generated password, and

store the coded password for use in connection with a secure operating system login access; and

apparatus from which the computer program is accessible by the computer system.

25. The computer program product of claim 24, wherein said computer program is further processable by the computer system for causing the computer system to:

display the stored coded password during an operating system login, wherein the displayed coded password is subject to being decoded with the use of a corresponding secure password provider, further wherein the secure operating system login is responsive to an input of a correctly decoded coded password for enabling access to the operating system as a function of the generated password and the operating system security module.

26. The computer program product of claim 24, wherein the prescribed password generation event includes at least one selected from the group consisting of a computer system power-up; a computer system re-boot; expiration of a prescribed time duration from an immediately preceding password generation event; restoration of a security level from a modified security level to a default security level, and occurrence of a secure operating system login access.

27. The computer program product of claim 26, wherein the modified security level of a password generation event includes at least one selected from the group consisting of a change in the security level within the dedicated application, a security level override within the dedicated application, and a one-shot security access within the dedicated application.

28. The computer program product of claim 24, wherein said computer program is further processable by the computer system for causing the computer system to:

search a username registry of the dedicated application upon the occurrence of the prescribed password generation event and remove any invalid usernames from the username registry, and

review privileges associated with respective valid usernames in the username registry and reset the privileges of the respective valid usernames to prescribed default settings.

29. The computer program product of claim 24, wherein generating the password includes generating the password for a service username.

30. The computer program product of claim 24, wherein the dedicated application includes a point of sale application in a fuel dispensing environment.